IN THE U.S. PATENT & TRADEMARK OFFICE

APPLICANT: MATTILA

SERIAL NO. 10/ _____ ATT. DOCKET: 540-017.2

FILED: 15 FEB. 2002 ART UNIT: 2130

FOR: METHOD FOR SETTING UP SECURE CONNECTIONS

PRELIMINARY AMENDMENT

15 FEB. 2002

COMMISSIONER FOR PATENTS
WASHINGTON, DC 20231

Sir:

Please amend the above-identified application by cancelling specification page 1 and substituting the attached new page 1.

REMARKS

A "version marked to show changes made" is enclosed. This change was necessary to remove an improper reference to the content of claim 1. Since the text of claim 1 has just been copied into the specification, no "new matter" issue is raised. At the bottom of page 1, a document cited on specification page 21 has been more fully cited, for the sake of clarity. If the Examiner detects any other informalities which would delay examination on the merits, a telephone call to Applicant's counsel is invited.

"Express Mail" Mailing Label No. **EV 005 525 861 US**
Date of Deposit: **FEB. 15, 2002**

I hereby certify that this document is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, P.O. Box 2327, ARLINGTON VA 22202.

Anita Schelmetic

Anita Schelmetic

Early examination and allowance of the present application are respectfully solicited.

Respectfully submitted,

Milton Oliver

Milton Oliver, Reg. # 28,333
Attorney for Applicant
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON, LLP
755 Main Street
P.O. BOX 224
MONROE, CT 06468-0224
Tel. (203) 261-1234
Fax (203) 261-5676

Attorney Docket # 540-017.2

E:\WP51\MMO\AMEND\540-0172.PAM

VERSION MARKED TO SHOW CHANGES MADE

METHOD FOR SETTING UP SECURE CONNECTIONS

FIELD OF THE INVENTION

The present invention is related to connections in IP (Internet Protocol) based networks, especially connections according to the IPSec protocol. Specifically, the invention is directed to a method [according to the first independent method claim.] for providing authentication for setting up secure connections between a plurality of network nodes comprising at least the steps of placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes by said first node, importing said collection by at least one other node than said first node, setting up of at least one secure connection by at least one of said at least one other node to a destination node whose certificate was imported as a part of said collection, and automatically accepting the authenticity of said destination node.

BACKGROUND OF THE INVENTION [Description of Related Art]

The basic protocols used in the Internet, namely the IP protocol (IP) and [TCP] Transmission Control Protocol (TCP), were created in an environment[,] where security was not a concern. Consequently, the security of a basic TCP/IP network is very poor if not practically nonexistent, if no further measures are taken. Many different approaches to improve the security of TCP/IP networks have been taken. One of the most popular techniques is the IPSec protocol (IPSec) which, at the time of writing this application, has established itself as an industry standard. The IPSec protocol provides a framework for establishing, using, and terminating secure connections over untrusted networks. The IPSec protocol does not strictly define which encryption methods are used. The encryption method is negotiated by the communicating parties during setup of a connection, which allows [the] change and improvement of encryption methods without breaking the IPSec protocol itself. IPSec is, by construction, a unidirectional protocol. For two-way communication, two communications channels must be set up, one for each direction. The IPSec protocol is described in further detail in the reference [IPSec] (RFC 2401 by S. Kent & R. Atkinson, November 1998) and in the documents referred to therein.

METHOD FOR SETTING UP SECURE CONNECTIONS

FIELD OF THE INVENTION

The present invention is related to connections in IP (Internet Protocol) based networks, especially connections according to the IPSec protocol. Specifically, the invention is directed to a method for providing authentication for setting up secure connections between a plurality of network nodes comprising at least the steps of

placing a collection of accepted certificates comprising at least one accepted certificate available for other nodes by said first node, importing said collection by at least one other node than said first node, setting up of at least one secure connection by at least one of said at least one other node to a destination node whose certificate was imported as a part of said collection, and automatically accepting the authenticity of said destination node.

BACKGROUND OF THE INVENTION

The basic protocols used in the Internet, namely the IP protocol (IP) and Transmission Control Protocol (TCP), were created in an environment where security was not a concern. Consequently, the security of a basic TCP/IP network is very poor if not practically nonexistent, if no further measures are taken. Many different approaches to improve the security of TCP/IP networks have been taken. One of the most popular techniques is the IPSec protocol (IPSec) which, at the time of writing this application, has established itself as an industry standard. The IPSec protocol provides a framework for establishing, using, and terminating secure connections over untrusted networks. The IPSec protocol does not strictly define which encryption methods are used. The encryption method is negotiated by the communicating parties during setup of a connection, which allows change and improvement of encryption methods without breaking the IPSec protocol itself. IPSec is, by construction, a unidirectional protocol. For two-way communication, two communications channels must be set up, one for each direction. The IPSec protocol is described in further detail in the reference (RFC 2401 by S. Kent & R. Atkinson, November 1998) and in the documents referred to therein.